Department of Homeland Security Daily Open Source Infrastructure Report for 21 July 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Orlando Sentinel reports marine experts say that a problem in the autopilot system on the Crown Princess likely caused the month−old cruise ship to tilt harshly to one side, injuring 240 passengers on Tuesday, July 18. (See item 14)
- The Washington Post reports two Georgia men, previously accused of contact with Islamic militants, have been charged in Atlanta with plotting attacks against civilian and military targets, including the U.S. Capitol and World Bank headquarters. (See item 36)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 20, BBC (UK)* — **Nuclear plant struck by jellyfish.** A nuclear power plant in Japan was forced to lower the output of its reactors after jellyfish blocked a filter in a seawater cooling system. Power from two reactors at Chubu Electric Power Co's plant in Hamaoka on Japan's Pacific coast had to be reduced after the water intake system shut down automatically. Workers removed the jellyfish mass and output later returned to normal. Output for the two reactors was reduced to between 60 and 70 percent of capacity for about three hours, the company said. Source: http://news.bbc.co.uk/1/hi/world/asia−pacific/5197846.stm

2. *July 20, Reuters* — **Alaska regulators push tighter rules after BP leaks.** Alaska regulators on Wednesday defended their oversight of BP Plc but advocated tighter rules after leaks forced the oil giant to shut down 12 oil wells this week. The wells shutdown in Alaska's North Slope region is the latest in a series of troubles for BP. State officials are working to tighten rules. The commission plans to rewrite oil field safety−valve regulations in order to address recent changes in field operations and improvements in measuring technology. The Alaska Department of Environmental Conservation is writing new regulations for oil pipeline operations. New rules that give the state oversight of the oil fields' flow lines and gathering lines are almost complete, a department official said. Those lines, which bring pumped oil to gathering and processing centers, have not been regulated in the past by the state or federal governments. Further, it is likely Alaska will tighten the state's one percent leak−detection standard, which requires companies to have an automated system to detect if one percent or more of daily volume of oil escapes.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/20/AR2006072000073.html

3. *July 20, Federal Energy Regulatory Commission* — **FERC Chairman statement on grid stability.** In a statement, Federal Energy Regulatory Commission (FERC) Chairman Joseph T. Kelliher said that earlier this week, electric utilities demand set records in New England, New York, PJM, Midwest ISO, California, and ERCOT. Within a 24−hour period, record demand levels were reached in seven regions of North America. According to Kelliher, the demand levels, occurring at the same time, across much of the country, represents the most severe test of the U.S. electric system since the August 2003 blackout. While there were a few short, localized outages, the bulk−power system succeeded in meeting customer demand. The Commission closely followed the events of the past week from two perspectives −− reliability and markets. On the transmission side, FERC followed both the fire that led to an outage of a major line from Manitoba to Minnesota and the Monday, July 17, return to service of one of the key ConEd cables serving Manhattan. That line returned just when it was needed most, even though it was not originally expected to return to service until some time in August.
   Chairman statement: http://www.ferc.gov/press−room/statements/kelliher/2006/07−20−06−kelliher−grid.asp
   Source: http://www.ferc.gov/

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 20, Tampa Bay Online (FL)* — **Fuel spill in Florida prompts road closure.** An 18−wheeler, which was carrying 8,000 gallons of gasoline, overturned on its side, spilling fuel onto a two−lane section of U.S. 41, about a mile north of State Road 52 in Pasco County, FL. With the tanker engulfed in flames, emergency crews rushed to the scene, shutting down the busy north−south thoroughfare in both directions shortly after 6 p.m. EDT.
   Source: http://www.tbo.com/news/metro/MGB059ULUPE.html

[Return to top]

Defense Industrial Base Sector

5. *August 01, National Defense* — **Overseas companies adapting to U.S. market needs.** With current commitments driving the high demand for military equipment, foreign companies perceive the U.S. defense market to be the proverbial pot of gold. Though breaking through American bureaucracy and politics to sell wares remains a daunting challenge, industry representatives at a recent international ground warfare conference in Paris say their businesses are becoming savvier at catering to U.S. defense needs. While European defense budgets remain on a downward slope, U.S. military spending has surged dramatically since the 9/11 attacks. Non−U.S. firms acknowledge that the Pentagon generally buys most major weapons systems from U.S. manufacturers, but many niche areas in the market increasingly are open to international competitors. From forming partnerships to custom−designing products, companies reveal they use multiple strategies to gain American clients.
   Source: http://www.nationaldefensemagazine.org/issues/2006/August/Ov erseascompanies.htm

6. *July 19, U.S. Army* — **Army continues prudent budget constraints in 2006, prepares for 2007.** Faced with the high costs of war, the Army currently plans to continue most of the spending restrictions it imposed prior to the Fiscal Year 2006 supplemental, which passed three weeks ago. These budget constraints will remain in place through the rest of this fiscal year, ending September 30, and into Fiscal Year 2007. Certain policies will be reviewed for possible modification, including civilian hiring and contracting limits, both of which were originally intended to be temporary means to preserve solvency in FY 2006. To conserve funding while awaiting passage of the main FY 2006 emergency supplemental appropriation, the Army significantly scaled back spending from its operations and maintenance account.
   Source: http://www4.army.mil/ocpa/read.php?story_id_key=9306

7. *July 19, U.S. Department of Defense* — **Army moving toward more joint, capable aircraft.** The idea of the services operating jointly with fewer aircraft platforms that share common features is the key to the modernization effort taking place throughout the military aviation community, the Army Aviation director said Wednesday, July 19. Army Brig. Gen. Stephen D. Mundt called the trend toward jointness a key driver in aviation modernization programs. But Mundt told Pentagon reporters he's concerned by budget cuts being eyed by Congress that threaten to set back the first major step toward that goal. These cuts could delay by as long as two years production of the Joint Cargo Aircraft (JCA) and ultimately, drive up the price, he said. They could also affect another major Army aviation program: the Armored Reconnaissance Helicopter. The JCA, being developed jointly by the Army and Air Force, will replace multiple other fixed−wing platforms. The request for proposals for the new aircraft is currently on the streets, Mundt said, and the Army hopes to begin adding the first JCAs to its fleet in fiscal 2007.
   Source: http://www.defenselink.mil/news/Jul2006/20060719_5693.html

[Return to top]

Banking and Finance Sector

8.

July 20, Finextra — **Rising number of SQL injection hack attacks against banks.** The past three months has seen a dramatic increase in the number of hack attacks attempted against banks, credit unions, and utility companies using SQL injection, a type of Web application probe. SecureWorks says from January through March, it blocked anywhere from 100 to 200 SQL Injection attacks per day. But as of April that number jumped from 1,000 to 4,000 to 8,000 per day. Jon Ramsey of SecureWorks says, "What makes this vulnerability so pervasive is that SQL Injection attacks can prey on all types of Web applications −− even those as simple as a monthly loan payment calculator or a 'signup for our customer newsletter' form...the criminal can potentially gain access to a bank or utility company's key customer databases containing social security numbers, account numbers, credit card numbers, e−mail addresses, etc."
Source: http://finextra.com/fullstory.asp?id=15602

9. *July 20, VNUNet* — **Scam e−mails promise cure for AIDS.** IT security watchers reported Thursday, July 20, that 419 scammers have been sending e−mails that claim to offer details of a cure for AIDS. The spam, which comes from a Yahoo e−mail address, claims that the '19 year−old correspondent' has found a herbal root that has successfully helped AIDS sufferers to recover. It also claims that hospitals have confirmed that patients are no longer HIV positive, and goes on to ask for help in bringing the cure to English−speaking markets. Sophos has warned that the e−mails are a ruse to steal personal details, and that the scammers behind the scam could use such information to steal money from bank accounts and commit identity fraud.
Source: http://www.itweek.co.uk/vnunet/news/2160684/aids−cure−419−sc am−emails

10. *July 20, Government Accountability Office* — **GAO−06−957T: Control Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper and Abusive Activity (Testimony).** In the wake of the 2005 hurricanes in the Gulf Region, the Government Accountability Office (GAO) and the Department of Homeland Security Office of Inspector General (OIG) initiated a number of audits and investigations addressing the federal government’s response to those events. Department of Homeland Security (DHS) cardholders made thousands of transactions related to hurricane rescue and relief operations. GAO, working with OIG, interviewed DHS personnel and reviewed purchase card policies and procedures to assess the control environment. GAO and OIG conducted statistical tests from a random sample of transactions and performed data mining on all DHS purchase card transactions for a 5−month period beginning in June 2005. GAO and OIG looked at all transactions in this period because the database did not distinguish hurricane related from routine purchases. GAO and OIG used the testing results to determine the extent of control weaknesses and identify instances of fraud, waste, and abuse. This testimony addresses whether DHS’s control environment and management of purchase card usage were effective; DHS’s key internal control activities operated effectively and provided reasonable assurance that purchase cards were used appropriately; and indications existed of potentially fraudulent, improper, and abusive or questionable purchase card activity at DHS.
Highlights: http://www.gao.gov/highlights/d06957thigh.pdf
Source: http://www.gao.gov/docsearch/repandtest.html

11. *July 19, Register (UK)* — **Online scammers love Web mail; easier to block accounts linked to spamming than fraud.** Online scammers favor easy to set−up Web mail accounts when perpetrating online fraud. Yahoo! accounts come first in a list of the top ten e−mail addresses used by online card scammers compiled by Early Warning UK, a scheme set up to help retailers avoid credit card fraud. Early Warning has established a database of scammers that includes

tens of thousands of entries. Subscribers to its CardAware protection service add hundreds more each month. Analysis of the last three years' data shows web mail services (such as Yahoo! and Hotmail) are preferred by crooks. E−mail addresses are a vital tool for scammers because without them it's very difficult to place orders online. Early Warning suggests Web mail providers are not being proactive enough in blocking accounts when presented with evidence that they're linked with fraudulent activity. Top 10 e−mail address domains linked to online fraud, according to Early Warning (1) Yahoo.com, (2) Yahoo.co.uk, (3) Hotmail.com, (4) AOL.com, (5) Hotmail.co.uk, (6) Parrot.com, (7) Postmaster.com, (8) Lycos.co.uk, (9) Lycos.com., and (10) Msn.com.
Source: http://www.channelregister.co.uk/2006/07/19/online_fraud_sur vey/

[Return to top]

Transportation and Border Security Sector

12. *August 01, National Defense Magazine* — **Mesh of technologies to provide maritime safety net.** While the Department of Homeland Security begins efforts to strengthen the nation's land borders, less publicized work continues on building a so−called virtual wall along U.S. coasts. And technological solutions are available. "If somebody could write me a check today, we could build it," said Guy Thomas, Coast Guard maritime domain awareness program science and technology advisor, referring to a system that would allow legitimate commerce through, while keeping bad guys out. Coast Guard Commandant Adm. Thad Allen has said the need to protect the nation's coasts should be a top priority. Researchers at the Coast Guard's annual innovation conference and exhibition presented solutions ranging from the use of remote sensing satellites to peer thousands of miles out to sea, to cutting edge sensors designed to detect underwater saboteurs inside ports. One system that has the green light and will begin operations in August is the vessel−tracking project at the Coast Guard maritime intelligence fusion center−Atlantic in Dam Neck, VA. The project will fuse multi−level intelligence data to help the Coast Guard and Navy track high interest vessels, according to Coast Guard Cmdr. John Wood, liaison to the Office of Naval Research.
Source: http://www.nationaldefensemagazine.org/issues/2006/August/Me shofTechnolog.htm

13. *July 20, Associated Press* — **Governor Romney closes another Big Dig tunnel.** Governor Mitt Romney has ordered closed the eastbound lanes of the Ted Williams Tunnel, which connects Boston to Logan International Airport. A spokesperson for the governor, Eric Fehrnstrom, says an initial assessment from the Turnpike Authority found no potential problems in the Big Dig tunnel that rose to the level of a public safety threat. But Fehrnstrom says the governor has decided to overrule that assessment. The eastbound lanes of the Ted Williams Tunnel bring traffic from South Boston to Logan Airport. It leads to the I−90 connector tunnel, which has been closed since last Monday, July 10, when ceiling panels fell and killed a Boston woman.
Source: http://www.wcsh6.com/news/article.aspx?storyid=38789

14. *July 20, Orlando Sentinel (FL)* — **Autopilot error suspected in tilting of cruise ship.** A glitch in the autopilot system on the Crown Princess likely caused the month−old cruise ship to tilt harshly to one side, injuring 240 passengers, marine experts said Wednesday, July 19. The 113,000−ton vessel was about 11 miles from Port Canaveral and headed for New York on

Tuesday, July 18, when it lurched 15 degrees to the port side, sending passengers and furniture flying, witnesses and officials said. The tilt was so extreme that even the casino's slot machines and the gymnasium's exercise equipment tipped over or slid across the floor, passengers said. The U.S. Coast Guard and the National Transportation Safety Board are investigating the cause of the mishap. Industry experts said severe listing is uncommon in cruise ships, but at least two other similar cases have happened in the past five years. Such vessels routinely use autopilot systems to set a desired course, which is then compared with compasses that direct the rudders. Any miscommunication between the systems could result in an abrupt stop or suddenly wild steering, experts said. Passengers were told on the ship that the problem was caused by a steering malfunction.
Source: http://www.sun−sentinel.com/news/local/florida/sfl−fcruise20jul20,0,3180545.story?coll=sfla−news−florida

15. *July 20, Pacific Business News* — **Continental Airlines profit: $198 million.** Continental Airlines doubled its profit in the spring quarter as passenger revenue rose 23 percent to more than $3 billion. "Our plan is working," said CEO Larry Kellner. "Everyone wins." Houston−based Continental, which flies to Hawaii from Guam, Los Angeles, Houston and Newark, said its operating income was $244 million, more than double the past year's levels despite fuel price increases above $200 million and a $60 million accrual for employee profit sharing.
Source: http://biz.yahoo.com/bizj/060720/1318381.html?.v=1

16. *July 20, USA TODAY* — **Lives saved as highways get cable.** A relatively low−cost safety device −− steel cable strung in highway medians −− is proving phenomenally effective at saving lives, perhaps more so than steel−beam or concrete barriers. Steel−beam, concrete and cable barriers all cut down on accidents in which cars cross over into oncoming traffic. Cable, however, also cuts down on the number of rebound accidents, in which a vehicle hits a barrier and bounces back into traffic. North Carolina, Missouri, Texas, Washington, California, and Utah are among the nation's leaders in installing median guard cable, according to the Texas Transportation Institute, a research body at Texas A&M University. The institute says 27 other states are following suit, including Florida, Wisconsin, Maine, and Idaho. Because cable barriers are considerably cheaper, states can install them in medians where motorists had no protection before. Most important, says Brian Chandler, a traffic−safety engineer with the Missouri Department of Transportation, median guard cables work. "When a vehicle hits a concrete barrier, it usually bounces back into traffic," he says. "But when you hit the guard cable, it gives 10 to 12 feet and helps absorb the force. The posts that hold the cable up are designed to break away. The cable stretches and wraps up the car in it."
Source: http://www.usatoday.com/news/nation/2006−07−19−highway−cable s_x.htm

[Return to top]

Postal and Shipping Sector

17. *July 19, Federal Times* — **Small firms strive to win USPS business.** When the U.S. Postal Service (USPS) adopted new procurement rules last year in an effort to streamline contracting, some expressed the fear that −− among other bad consequences −− small businesses would find it harder to compete for Postal Service contracts. But the USPS says the amount of money

going to small businesses, women−owned businesses, and minority−owned businesses has not fallen at all and remains a healthy percentage of all agency dollars contracted. “Over the past three years, the [small] business percentages [including small minority− and women−owned businesses] have averaged a steady 47 percent,” said Janice Williams−Hopkins, Postal Service program manager for supplier diversity. In fiscal 2005, total contractual activity −− money spent on goods and services that does not include contracts with foreign countries, educational institutions or mandatory spending −− was $8.4 billion. Of that, $3.8 billion went to small businesses.
Source: http://federaltimes.com/index.php?S=1952648

[Return to top]

Agriculture Sector

18. *July 20, U.S. Department of Agriculture* — **New bovine spongiform encephalopathy surveillance program announced.** U.S. department of Agriculture (USDA) Secretary Mike Johanns announced Thursday, July 20, that the USDA will soon begin transitioning to an ongoing bovine spongiform encephalopathy (BSE) surveillance program that corresponds to the extremely low prevalence of the disease in the U.S. The ongoing BSE surveillance program will sample approximately 40,000 animals each year. Under the program, USDA will continue to collect samples from a variety of sites and from the cattle populations where the disease is most likely to be detected, similar to the enhanced surveillance program procedures. The new program will not only comply with the science−based international guidelines set forth by the World Animal Health organization (OIE), it will provide testing at a level ten times higher than the OIE recommended level. Once the ongoing surveillance program begins, USDA will periodically analyze the surveillance strategy to ensure the program provides the foundation for market confidence in the safety of U.S. cattle.
Ongoing BSE surveillance plan: http://www.aphis.usda.gov/newsroom/hot_issues/bse.shtml
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/07/0255.xml

19. *July 20, Agricultural Research Service* — **New gooseberry resists diseases.** Agricultural Research Service (ARS) scientists have developed and released a new disease− and pest−resistant dessert gooseberry called "Jeanne." This new late−fruiting gooseberry was developed by ARS scientists at the National Clonal Germplasm Repository (NCGR) in Corvallis, OR. Gooseberry production is limited in the U.S., partially due to restrictions imposed in the last century. Like other Ribes species, gooseberries are generally susceptible to white pine blister rust. While the disease causes them little harm, it can be devastating to pine trees. Jeanne gooseberries are highly resistant to white pine blister rust and to powdery mildew, the biggest disease threat to U.S. gooseberry production.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

20. *July 17, WJZ (Maryland)* — **Tests ordered, charges filed against hog farmers.** A father and son are facing several charges, including feeding garbage to pigs and animal cruelty, following raids on their Carroll, MD, farm where several hogs have tested positive for trichinosis. State agricultural officials face growing concerns about the spread of trichinosis after three Carroll County pigs tested positive for the parasitic disease. Officials from the state Department of

Agriculture said that the pigs were from a farm in New Windsor. Carroll Schisler, 60, the farm's owner, and his son, Carroll Schisler Jr., 34, were arrested on a 19−count indictment that also included federal charges of operating a slaughterhouse without a license. The arrests followed raids in March and April, in which investigators discovered piles of dead animals and livestock feeding on garbage. At that time, state agriculture officials said a malnourished pig taken from the farm tested positive for trichinosis. Now, officials confirm that three more pigs believed to have wandered from the farm have tested positive.
Trichinosis information: http://www.cdc.gov/ncidod/dpd/parasites/trichinosis/factsht_trichinosis.htm
Source: http://wjz.com/topstories/local_story_198153341.html

[Return to top]

Food Sector

21. *July 20, USAgNet* — **Cranberries fight food−borne illness.** New data from the University of Maine has shown that cranberries may offer defense against microbial pathogens in ground beef. A compound in cranberries has the unique ability to inhibit the growth of harmful bacteria, the researchers found. The researchers have observed that adding natural cranberry concentrate to raw minced beef significantly reduced the growth of common food−borne pathogens, including Salmonella, Listeria and E. coli. In the University of Maine trials, ground beef samples inoculated with four pathogens were treated with cranberry concentrate or sterile water (control) and kept at 21−degrees C or 7−degrees C. Pathogens and total viable bacteria were enumerated on days one, three, five, and seven. Results showed that, compared to the control, cranberry concentrate significantly inhibited food−borne pathogens in ground beef at both temperatures.
Source: http://www.usagnet.com/story−national.cfm?Id=1402&yr=2006

[Return to top]

Water Sector

22. *July 20, Houston Chronicle* — **San Antonio, Texas, area hit with restrictions on water use.** For the first time since 2000, mild but mandatory water−use restrictions were imposed in a seven−county area beginning Thursday, July 20, as the Edwards Aquifer plummeted below the point that triggers forced conservation measures. The ban on wasteful practices and limits on routine uses will be in place for at least a month under the emergency declaration by the Edwards Aquifer Authority. Officials said they have little control over how much water enters the underground formation, but they can influence how much is removed by homeowners and businesses in Bexar and Medina counties and portions of Atascosa, Comal, Guadalupe, Hays, and Caldwell counties.
Source: http://www.chron.com/disp/story.mpl/metropolitan/4058911.htm l

[Return to top]

Public Health Sector

23. *July 20, Agence France−Presse* — **Bulgaria gets its first case of bird flu in poultry.** Bulgaria has registered its first case in poultry of the bird flu virus, Agriculture Minister Nihat Kabil has said. He said the virus had been detected near Djebel in the south of the country in a preliminary test by a Sofia laboratory. He said he had ordered the destruction of all poultry and poultry products in the region. The Sofia laboratory will give a definitive ruling within four days on whether it is the H5NI strain. Four cases of H5N1 were registered in swans in northern Bulgaria in February.
Source: http://news.yahoo.com/s/afp/20060720/hl_afp/healthflubulgaria_060720154204;_ylt=Au7RM887iLxA4v8JFmaynAGJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

24. *July 20, New York Times* — **In the bird−flu fight, Indonesia falls behind.** Indonesia is poised to surpass Vietnam as the country hardest hit by avian flu. And while Vietnam has not had a single human case or poultry outbreak this year, public health officials and experts say the situation in Indonesia is likely to get worse. Indonesia received word from a Hong Kong laboratory that a 44−year−old man who died near Jakarta had tested positive for the H5N1 virus, the Indonesian Health Ministry said Thursday, July 20. That brought number of confirmed bird flu deaths in Indonesia to 42 since the first human case was confirmed a year ago, equal to the toll in Vietnam. The flu is ubiquitous in thousands of Indonesian backyard flocks, and appears to be killing more birds every month, increasing the likelihood of human cases. Although the H5N1 flu came relatively late to Indonesia, it soon spiraled out of control, and deaths have mounted quickly. Unlike Thailand, which quenched outbreaks by killing millions of chickens, or Vietnam, which used mandatory vaccination, Indonesia has tried a mix of limited culling and vaccinating in rings around the cull −− so far, with little success.
Source: http://www.iht.com/articles/2006/07/20/news/flu.php

25. *July 18, Purdue University* — **Host protein triggers infection by smallpox−related viruses.** For the first time, scientists have shown that a protein in the nucleus of victims' cells triggers progression of smallpox−related illnesses, a finding that could help prevent use of such viruses as bioterrorism weapons. Purdue University scientists found that poxviruses move to the second and third stages of development by recruiting a protein, called TATA−binding protein, in the nucleus of mammals' cells. "This protein is required for activation of the middle− and late−stage poxvirus genes," said Steven Broyles, a Purdue biochemistry professor. "In the past, we were just groping around. We now have a model for how the poxvirus growth process is orchestrated."
Source: http://news.uns.purdue.edu/UNS/html4ever/2006/060717.Broyles .poxvirus.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *July 20, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Storm Beryl: At 5:00 am EDT Thursday July 20, the center of Tropical Storm Beryl was located near latitude 37.8 north, longitude 73.2 west or about 210 miles south of New York City and about 295 miles south−southwest of Nantucket, MA. A tropical storm watch remains in effect for southeastern Massachusetts from Plymouth to Woods Hole, including Cape Cod, Nantucket Island, and Martha's Vineyard. Additional watches or warnings may be required for portions of Long Island and the New England coast. Beryl is moving toward the north at 9 mph. A turn toward the northeast and a faster forward speed are expected during the next 24 hours. This motion could bring the center of Beryl near the southeastern coast of Massachusetts Thursday night or Friday morning. Maximum sustained winds are near 60 mph with higher gusts.
For the latest information: http://www.nhc.noaa.gov/
Earthquake Activity: A Moderate 5.0 magnitude earthquake occurred offshore Northern California at 7:41 am EDT Wednesday, July 19. The epicenter was 198 miles northwest of Sacramento, CA, at a depth of 12.9 miles. No tsunami was generated.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat072006.shtm

27. *July 19, Mercury News (CA)* — **Disaster planning with pets in mind.** For the first time, the Red Cross will hold a disaster−planning workshop this weekend that includes preparations for family pets. "We learned from the incidents during Katrina that we needed to come up with a plan that educates families on how to deal with pets," said Elizabeth Leslie, spokesperson for the Santa Clara Valley, CA, Chapter of the American Red Cross, which is sponsoring the San Jose event. Information sessions during the workshop at the Santa Clara County fairgrounds will include tips on how to provide for pets during an emergency, the benefits of microchipping and including pets in families' emergency plans. Representatives from emergency agencies and animal−welfare groups will be available to answer questions.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/150717 81.htm

28. *July 19, CBS 5 (CA)* — **Grand Jury Report: San Mateo County residents not prepared for disaster.** A San Mateo County, CA, civil grand jury report released Wednesday, July 20, found that, while county and city officials are taking steps toward preparing for the next big Bay Area disaster, the county's residents are not doing enough to prepare themselves. Lt. John Quinlan, director of the San Mateo County Office of Emergency Services (OES) and Homeland Security, agreed, stating that the grand jury's observation of the small number of Community Emergency Response Team (CERT) participants in the county is an issue that has not gone unnoticed by the OES. According to the report, every city in the county, excluding Burlingame, Millbrae and San Bruno, has an active CERT program. As part of its report the grand jury recommended that each city council within the county promote its CERT program and strive to train five percent of its households.
To view the report: http://www.sanmateocourt.org/grandjury/2005/reports/Disaster_P_Training_Residents.pdf
Source: http://cbs5.com/localwire/localfsnews/bcn/2006/07/19/n/HeadlineNews/DISASTER−PREPAREDNESS/resources_bcn_html

[Return to top]

Information Technology and Telecommunications Sector

29. *July 20, Federal Computer Week* — **IT council praises DHS.** The newly established Information Technology Sector Coordinating Council (IT SCC) is praising the Department of Homeland Security's (DHS) National Infrastructure Protection Plan for its "pragmatic and progressive approach to the relationship between industry and the government and their mutual goals of critical infrastructure protection," according to a statement issued Wednesday, July 19. The IT SCC, an industry group founded in January, also lauded DHS' current focus on physical security issues, "enhancing programmatic attention to the role of cybersecurity as a foundational pillar for overall critical infrastructure security," according to the statement.
Source: http://www.fcw.com/article95340−07−20−06−Web

30. *July 20, Register (UK)* — **Trojan poses as Google Toolbar.** Spam messages that began circulating on Wednesday, July 19, attempt to trick users into visiting a maliciously constructed Website, disguised to resemble the genuine Google Toolbar site, reports UK−based net security firm SurfControl. Users who accept a offer to download "Google Toolbar" software from the bogus site will find themselves installing a Trojan which turns their machines into zombie clients, controlled by hackers.
Source: http://www.channelregister.co.uk/2006/07/20/google_toolbar_t rojan/

31. *July 19, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−200A: Oracle products contain multiple vulnerabilities.** Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial−of−service.
Systems Affected: Oracle10g Database; Oracle9i Database; Oracle8i Database; Oracle Enterprise Manager 10g Grid Control; Oracle Application Server 10g; Oracle Collaboration Suite 10g; Oracle9i Collaboration Suite; Oracle E−Business Suite Release 11i; Oracle E−Business Suite Release 11.0; Oracle Pharmaceutical Applications; JD Edwards EnterpriseOne, OneWorld Tools; Oracle PeopleSoft Enterprise Portal Solutions.
Solution: Apply the appropriate patches or upgrade as specified in the Oracle Critical Patch Update. Note that this Critical Patch Update only lists newly corrected issues. Updates to patches for previously known issues are not listed.
Oracle Critical Patch Update − July 2006:
http://www.oracle.com/technology/deploy/security/critical−pa tch−updates/cpujul2006.html
Source: http://www.uscert.gov/cas/techalerts/TA06−200A.html

32. *July 19, Security Focus* — **Retired: Cisco Security Monitoring Analysis and Response System multiple vulnerabilities.** Cisco Security Monitoring, Analysis and Response System (CS−MARS) is prone to multiple vulnerabilities. Analysis: To include privilege−escalation, arbitrary command−execution, and information−disclosure issues. An attacker could exploit these issues to retrieve potentially sensitive information and possibly execute arbitrary commands with Super User privileges. This may facilitate a remote compromise of affected computers.
Vulnerable: Cisco CS−MARS 4.1.5; Cisco CS−MARS 4.1.3; Cisco CS−MARS 4.1.2; Cisco CS−MARS 4.1.
Solution: Fixes are available. Refer to the Cisco advisory for details:

http://www.securityfocus.com/bid/19071/references
Source: http://www.securityfocus.com/bid/19071/references

33. *July 19, CNET News* — **Microsoft irons out security patch.** Microsoft on Tuesday, July 18, fixed two glitches related to one of its recently released security patches. One of the problems, in security bulletin MS06−034, led some people to be repeatedly offered the same patch via Microsoft's update delivery tools. A second glitch affected people running Windows Server 2003 Service Pack 1 in which the MS06−034 patch would not be offered to users if the initial update failed to install.
Source: http://news.com.com/Microsoft+irons+out+security+patch/2100−1002_3−6096179.html?tag=nefd.top

34. *July 19, Associated Press* — **Agencies to teach cybersecurity protection.** Federal scientists who study how hackers try to break into computer−based controls for nuclear reactors and other automated industrial systems are passing the secrets on to the private operators of such facilities. The U.S. Department of Energy and U.S. Department of Homeland Security will sponsor free classes in protecting remote controls of critical infrastructure during an international cybersecurity summit in Las Vegas September 28−30. Researchers from the Idaho National Laboratory will demonstrate cybersecurity attacks on Supervisory Control and Data Acquisition, or SCADA, networks that regulate electrical−supply systems and other automated industrial controls of potential terrorist targets, such as railroads, chemical plants and hydroelectric dams.
Source: http://www.nytimes.com/aponline/technology/AP−Cybersecurity−Protection.html?_r=1&oref=slogin

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

VU#936945: Microsoft PowerPoint contains an unspecified remote code execution vulnerability. http://www.kb.cert.org/vuls/id/936945

US−CERT strongly recommends the following until an update, patch, or more information becomes available:

Do not open attachments from unsolicited email messages.

Install anti virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments. http://www.us−cert.gov/cas/tips/ST04−010.html

US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	44139 (−−−), 1026 (win−rpc), 4672 (eMule), 445 (microsoft−ds), 113 (auth), 6881 (bittorrent), 32790 (−−−), 80 (www), 139 (netbios−ssn), 6346 (gnutella−svc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

35. *July 20, Providence Journal (RI)* — **Rhode Island is focusing on fixing a weak dam−safety program.** There are more than 600 dams in Rhode Island. And any failures could cause widespread destruction. It is not clear how many people in Rhode Island's inland communities are at risk. Unlike in coastal zones, where flood−prone areas are clearly mapped, the precise mapping of homes and businesses threatened by dam failures has in most cases not been done. Residents are being advised to plan ahead and assess their own risk. Because of a recently

enacted state law, more help is on the way to assess risks. But for this hurricane season, homeowners are on their own. "We didn't get into dams," said Robert Warren, executive director of the Rhode Island Emergency Management Agency. "But the locals should know who needs to evacuate. The towns should know. People seem to think government is going to take care of everything. It can't." A total of 16 dams are officially classified as "high hazard," meaning "more than a few" people would be killed if they failed. Another 41 dams are classified as "significant hazard," meaning "probable loss of a few lives" and appreciable property.
A copy of the state's latest list of dams and reports on inspections can be found by going to http://www.dem.ri.gov/ and clicking on "Compliance and Inspections" and then "Dam Safety Program Annual Reports −− 2005."
Source: http://www.projo.com/news/content/projo_20060720_dams20.170e149.html

[Return to top]

General Sector

36. *July 20, Washington Post* — **Georgia pair charged in plot to strike Capitol, World Bank.** Two Georgia men previously accused of contact with Islamic militants were charged with plotting attacks against civilian and military targets, including the U.S. Capitol and World Bank headquarters, according to an indictment handed up on Wednesday, July 19, in Atlanta. The new charges also allege that Syed Haris Ahmed, 21, and Ehsanul Islam Sadequee, 19, underwent "physical and rudimentary paramilitary training to prepare for participation in violent jihad" both overseas and in northwest Georgia. The four−count indictment, returned by a federal grand jury in Atlanta, adds to previous allegations against Ahmed and Sadequee, who had been accused of traveling to Toronto in March 2005 to discuss attacks in the United States with unidentified "like−minded Islamic extremists." The FBI also has said the men may have had limited contact with 17 men arrested in Canada in June in connection with a terrorism plot against targets in that country. Ahmed is a naturalized U.S. citizen born in Pakistan; Sadequee is a U.S. citizen of Bangladeshi descent who was born in Fairfax County, VA, but moved to the Atlanta area with his family when he was young, officials said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/19/AR2006071901748.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer